

## CLAIMS

1. A method for calculating the product  $P$  of a first number  $X$  and a second number  $Y$ , modulo  $N$ , where  $Y$  is partitioned into  $j$  words each of length  $p$  bits, and  $X$  has a length  $(m + n)$  bits, comprising the steps of:
- 5     a)     initialising (21) a product register,  $P$
- b)     loading a first one of the  $j$  words of  $Y$  into a multiplier;
- c)     multiplying (23) the loaded word of  $Y$  by  $X$  to form an intermediate product  $T$ ;
- 10     d)     updating (24) the product register  $P$  with the sum of  $T$  and  $P * 2^p$ ;
- e)     reducing (25) the contents of the product register  $P$  by subtraction of a value  $P_H (N' / 2)$ ;
- f)     loading a successive one of the  $j$  words of  $Y$  into the multiplier and repeating steps c) to e) for each one of the  $j$  words of  $Y$ ,
- 15             wherein  $N'$  is an integer multiple of  $N$ , and the value  $N'$  is selected such that the  $(m - 1)$  most significant bits are equal to '1', and the least significant bit is '0', and
- wherein  $P_H$  is selected as the  $(p + 2)$  most significant bits of  $P$  in the register.
- 20
2. The method of claim 1 in which the second number  $Y$  is also  $(m + n)$  bits in length.
3. The method of claim 1 or claim 2 further including the step of
- 25     selecting  $m \geq p + 3$ .
4. The method of any preceding claim further including the step of selecting  $(m + n)$  as a multiple of  $p$  bits.
- 30
5. The method of any preceding claim further including the step of using a  $(p + 2) * p$  multiplier (45) to perform the multiplying step and for deriving the value  $P_H (N' / 2)$ .

6. The method of any preceding claim in which the first one of the  $j$  words of  $Y$  loaded into the multiplier is the most significant word, and successive ones of the  $j$  words are loaded in decreasing order of significance.

5

7. The method of any preceding claim carried out in a pipelined processing architecture, in which the multiplication step (23) for a successive cycle through steps c) to e) commences prior to completion of the subtraction step e) (25) of a preceding cycle.

10

8. A processor (40) for calculating the product  $P$  of a first number  $X$  and a second number  $Y$ , modulo  $N$ , where  $Y$  is partitioned into  $j$  words each of length  $p$  bits, and  $X$  has a length  $(m + n)$  bits, comprising:

- a) initialisation means for initialising a product register,  $P$  (41);
- 15 b) loading means (42Y, 43Y, 44Y) for loading a first one of the  $j$  words of  $Y$  into a multiplier (45);
- c) a multiplier (45) for multiplying the loaded word of  $Y$  by  $X$  to form an intermediate product  $T$ ;
- d) update means (44R) for updating the product register  $P$  (41) with  
20 the sum of  $T$  and  $P * 2^p$ ;
- e) reduction means (45) for reducing the contents of the product register  $P$  by subtraction of a value  $P_H (N' / 2)$ ;
- f) control means (42Y, 43Y, 44Y) for loading successive ones of  
25 the  $j$  words of  $Y$  into the multiplier (45) and repeating the functions of the multiplier, the update means and the reduction means for each one of the  $j$  words of  $Y$ ,

wherein  $N'$  is an integer multiple of  $N$ , and the value  $N'$  is selected such that the  $(m - 1)$  most significant bits are equal to '1', and the least significant bit is '0', and

30 wherein  $P_H$  is selected as the  $(p + 2)$  most significant bits of  $P$  in the register.

9. The processor of claim 8 in which the second number Y is also (m + n) bits in length.

10. The processor of claim 8 or claim 9 in which  $m \geq p + 3$ .

5

11. The processor of any one of claims 8 to 10 in which (m + n) is an integer multiple of p bits.

12. The processor of any one of claims 8 to 11 in which the multiplier (45) is a  $(p + 2) * p$  multiplier also adapted to provide the value of  $P_H (N' / 2)$  to the reduction means (45).

10

13. The processor of any one of claims 8 to 12 in which the loading means (42Y, 43Y, 44Y) is adapted to load the most significant word of Y as the first one of the j words of Y loaded into the multiplier (45), and successive ones of the j words are loaded in decreasing order of significance.

15

14. The processor of any one of claims 8 to 13 implemented in a pipelined processing architecture, in which the multiplier (45) commences the multiplication operation to obtain a new value of T for a successive cycle prior to the reduction means (45) completing the reduction of the contents of P for a preceding cycle.

20

15. A computer program product, comprising a computer readable medium having thereon computer program code means adapted, when said program is loaded onto a computer, to make the computer execute the procedure of any one of claims 1 to 7.

25